SECURONIX™

DATASHEET

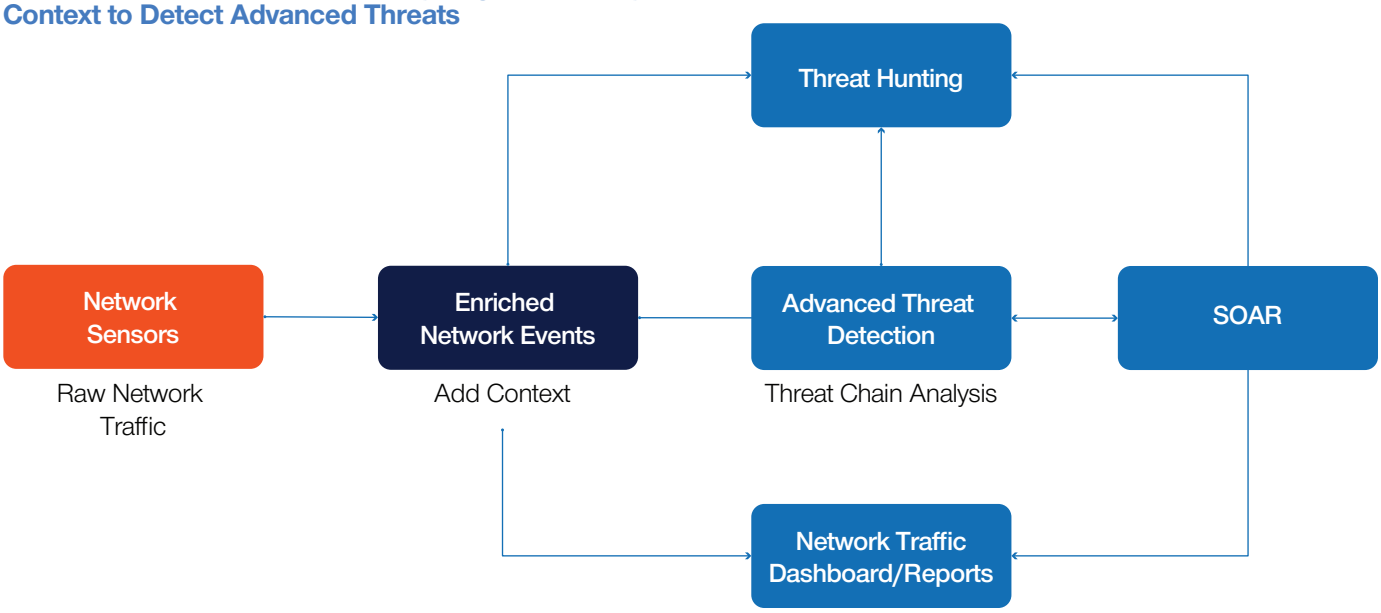
Securonix Network Detection and Response

Advanced Threat Monitoring Combining Network Traffic, Security Logs, Entity Context

Customers today struggle to detect the sophisticated slow and low attacks which require monitoring a blend of network traffic activity, user actions, and system behavior patterns. Stand-alone network traffic analysis tools can monitor traffic and detect network traffic anomalies, however, such anomalies without user and system context are less actionable and just add to the noise.

Securonix provides you with a single platform that monitors and correlates network traffic events, security events, and user activities to detect the most advanced threats.

Combine Network Traffic, Security Logs, and Entity Context to Detect Advanced Threats

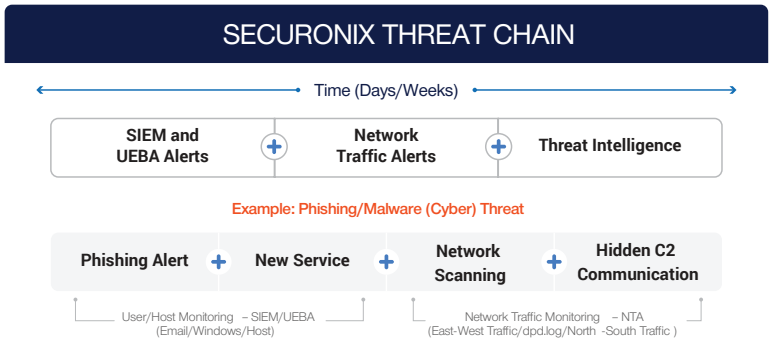


With Securonix Network Detection and Response (NDR), Securonix Next-Gen SIEM can provide customers with a single platform that monitors and correlates network traffic events, security events, and user activities, using built-in user and entity behavior analytics (UEBA) to detect the most advanced threats.

Securonix NDR Benefits

- Identify advanced threats that standalone NDR or security information and event management (SIEM) solutions are not able to detect.
- Improve efficiency and lower the operational overhead related to training and enablement when you only need to use a single console and database for all events.
- Rapid investigation and response using text-based search and link analysis on context enriched events and built-in security orchestration, automation, and response (SOAR) capabilities.
- Reduce false positives by over 90% by prioritizing threats using Securonix threat chains that span across network and security events.

Detect and Prioritize Advanced Threats with Network Traffic Analysis



Advanced cyberattacks are usually slow and low and involve multiple steps. Detecting such threats requires monitoring and correlating indicators of compromise (IOC) across event sources.

Securonix uses threat chain analytics to stitch together IOCs across network traffic, security events, and user actions to detect advanced threats. Securonix threat chains are based on industry standard kill chain models such as the MITRE ATT&CK framework.

Straightforward Threat Hunting

Securonix Spotter enables blazing-fast threat hunting using natural language search.

The Securonix Investigation Workbench allows you to search for threat actors or indicators of compromise with visual pivoting available on any entity in order to develop valuable threat context.

Visualized data can be saved as dashboards or exported in a standard data format.

Improve Network Traffic Visibility

Data insights include reports on network traffic with built-in, shareable dashboards. Securonix also includes out of the box reports and the ability to create custom visualizations and reports as needed.

For more information about Securonix NDR visit www.securonix.com/products/network-detection-and-response/.

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000

14665 Midway Rd. Suite #100, Addison, TX 75001 | ©2018 Securonix